ONREUR Report

9-11-C

International Open Systems Conference

J.F. Blackburn

14 August1989

Approved for public release; distribution unlimited

Office of Naval Research European Office

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 9-11-C	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Office of Naval Research European Office 6b. OFFICE SYMBOL (If applicable) (ONREUR)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Box 39 FPO NY 09510-0700	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)
International Open Systems Conference

12. PERSONAL AUTHOR(S)
J.F. Blackbrun

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Conference	FROM _____ TO _____	14 August 1989	16

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	
05	02		Information Science

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

At the International Open Systems Conference, papers were given on Open Systems Interconnection Perspectives, International Aspects of Open Systems Interconnection, Conformance Testing and Certification, Standard Issues, and Migration Strategies.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Ms. Connie R. Orendorf	22b. TELEPHONE (Include Area Code) (44-1)409-4340 22c. OFFICE SYMBOL 310

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

☆ U.S. Government Printing Office: 1986—607-044

Contents

International Open Systems Conference

Introduction

The sixth International Open Systems Conference was held at the Queen Elizabeth II Conference Centre, London, March 21 and 22, 1989. It was attended by 118 delegates, about two-thirds of whom were from the U.K. and the rest mainly Western Europe but with a few from the U.S. and Canada. The conference covered Open Systems Interconnection (OSI) Perspectives, International Aspects of OSI, Conformance Testing and Certification, Standard Issues, and Migration Strategies.

Summaries of the papers given are included in the following sections.

OSI Perspectives

Chairman, Adrian Stokes, Principal Consultant, NHS Information Management Center.

OSI Present and Future - A Systems Approach, Bryan Wood, Principal Consultant, SEMA Group and IT Standards Unit, Department of Trade and Industry. We need to establish the requirements for OSI standards in order to set objectives for standardization, hence be able to evaluate the OSI program. A systems approach is needed; e.g., the normal disciplines of system thinking applied to the specification of requirements for standards and to the development of the standards themselves.

The Basic Reference Model of OSI (ISO7498) sets out the objectives: "to define a set of standards which allow real open systems to cooperate" where these standards are concerned with "the interconnection aspects of cooperation between systems;" defines a high level system model of the objectives (the OSI environment); defines general principles to partition the objectives to allow partitioning of the solution (layering, step-by-step building of functionality); and makes specific choices of partitioning of functionality (the specification of seven layers), aiming for simplification, and avoidance of duplication of function.

Despite this original direction, the system view has to some extent been obscured. There are several areas within the original OSI program or evolving from it where it is becoming critically important to establish the system context. These include:

1. The lower layers of the OSI Reference Model-Provision of the transport service. The variety of scenarios is very large. Which are the major scenarios to be covered? And which of them are the most significant? Is it a real medium or long-term requirement that systems should be able to negotiate on protocol support to provide a requested quality of service?

2. Application layer standard. The standards for the application layer are concerned with supporting interworking between applications in end systems. Consequently, they must reflect the purpose and meaning of the communications for the applications involved. Requirements that must be reflected in the standards include: two systems may be involved in a given distributed application, and the applications must share a common view of the purpose of their interworking.

There are important characteristics of application layer standards not currently reflected in the reference model: they may define interactions between more than two systems, together with rules relating to these separate interactions; they include specifications that relate to the meaning of interactions in terms of the ultimate purpose that they serve and/or in terms of a specific information processing activity; and, in general, they relate to services offered by an application in one end system to an application in the end system communicating with it.

3. System Building. Formally, OSI standardization had as its objective the development of protocols for information exchange and interaction between parts of open systems without concern for the meaning of these protocol exchanges within a system. Whereas in practice, OSI standards have been seen as a basic tool for building distributed systems using components from different suppliers such as the DMA/address generator (MAP) and TOP specifications, there needs to be a clear specification of the kinds of system that are of major concern.

4. Major issues for a systems approach. We must consider the objective of OSI standardization. Is it the establishment of a worldwide community of computer systems, able to communicate in certain prescribed ways by virtue of their adherence to OSI standards? Or is it to provide specifications which allow information technology (IT) systems to be built from component computer systems of different manufacturers and operating systems?

In fact, OSI standards are seen as addressing both objectives, but its implications have not been examined. What is the necessary scope of standards for building systems? It is clear that distributed systems may involve more than standards for communication. Database standardization is needed to allow database facilities to be implemented independently in different components of the system while retaining consistency across the system and the capability for data exchange. Standardization of the operating system environment is needed

---

Dr. Blackburn is the London representative of the Commerce Department for Industrial Assessment in Computer Science and Telecommunications.

to allow flexibility and evolution of the configuration of the system and of the applications it supports. Also, standards are needed to cover the presentation of information to allow flexibility and evolution of the system.

Standards are needed in management, security and recovery to support a range of system policies. Since the range is large, it is essential to identify the major choices that are required in order to provide realistic and realizable objectives.

There is also a need for IT users to develop appropriate application systems models that reflect their system requirement and from which statements of standards requirements can be derived.

Future Developments of an OSI Architecture

Bernard Jones, Open Systems Group, Central Computer and Telecommunications Agency (CCTA), U.K. The CCTA (a part of the Treasury) has had a long standing commitment to OSI, dating back to 1984. In February 1988, the European Community (EC) made the specification of OSI and communications standard mandatory for public sector procurement within the EC.

The CCTA published a "Catalogue of Standards" in 1988 that provides an annotated list of the most recent and frequently used standards, highlighting those covered by European legislation. In 1988, CCTA published an OSI products review in collaboration with the Department of Trade and Industry (DTI). However, while users select and manufacturers implement different subsets, OSI products will be compatible on paper but rarely interconnect in practice.

Government Open Systems Interconnection Profile (GOSIP) Project. In August 1986, CCTA set up the GOSIP project, with the objectives to facilitate procurement and acceptance testing of communications-based products; ensure that different and separating procured departmental systems can interwork to an assured level of functionality; and provide a clear specification to manufacturers on which to base strategic project development.

GOSIP was published as Version 3.0 in January 1988 and it includes a management summary and introduction, the specification for the technically minded, and a procurement handbook for project officers.

The impact of GOSIP has been enormous. Following the U.K. initiative, the U.S. has created a profile, also called GOSIP, that is aimed at the U.S. administration. This will become mandatory for a number of U.S. government departments. Other governments are developing profiles of their own including Canada, Sweden, Singapore, Korea, Australia, and Norway. Now a European profile called EPHOS is being developed by the U.K., France, and Germany. The proposal to produce a procurement handbook suitable for use within all three administrations and meeting the legislative requirements of the EC was adopted. Discussions are now proceeding with the EC on funding for the project.

The GOSIP profile will be progressively updated in line with customer demand, the availability of products and emerging standards in the open systems environment.

International Aspects of OSI

Chairman, Jacob F. Blackburn, Industry Assessment Officer, U.S. Embassy London.

The subject of OSI is indeed international. Speakers in this session will concentrate on OSI and its impact in Europe and Canada with some particular considerations in France with respect to value added network services.

As is well known, there are a good many organizations concerned with standards that take a global view of OSI. These include the principal instigator of OSI, the International Organization for Standardization (IOS), as well as the CCITT (part of ITU); the Corporation for Open Systems (COS); the International Electrotechnical Commission (IEC) and the International Federation for Information Processing (IFIP).

There are also regional standards groups and national standards groups which I am sure will be discussed by the three speakers in this session. One important impact of OSI has been to cause unprecedented concentration on standards, not only in telecommunications but also on computers as well. The merging of these two industries has led to the need for intercommunications and interoperation of computer systems widely scattered throughout the world. This leads to the desirability for common standards in architecture and protocols in communication, and in operating systems and computer languages in computing.

European Research Coordination Agency's (EUREKA's) project Cooperation for Open Systems Interconnection Networking in Europe (COSINE) is expected to bring about greater standardization of data communications in Europe. According to plans, it will enable any researcher at a university or commercial laboratory in Europe to work together with scientists elsewhere, whatever the type of computer being used. The COSINE can be of direct and immediate use to all EUREKA projects, the EC's European Strategic Program for Research and Development in Information Technologies (ESPRIT) program, and Research in Advanced Communications for Europe (RACE) program as well as to CERN and the European Space Agency.

Reseau Associie's pour la Recherche Europeane (RARE) is in charge of the technical implementation of COSINE. European Academic and Research Network (EARN) and EUNET, two major computer networks for researchers in Europe will work with RARE to achieve a

single data communications infrastructure in accordance with the OSI standards.

I believe the speakers in this session will provide us with considerable insight into the initiatives being undertaken in Europe and North America. We have two European speakers and one Canadian.

European Initiatives for OSI, Georgia Efthymiopoulou, Commission of the European Communities. The Commission of the European Communities (Communities) having recognized at an early stage the strategic importance of information technology and the key role and value of OSI standards has formulated a coherent Communities policy on OSI as part of its overall IT strategy.

The evolution of information technology brought about a shift of emphasis from a largely centralized approach to a highly distributed one resulting in bringing intelligence and processing power closer to the end user. This requires an increasing flow of information across communication networks, which in turn requires network standards. The cumulative effect of worldwide user initiatives such as MAP, TOP, EMUG, Open Systems Interconnection Technical and Office Protocols (OSITOP) and GOSIP has contributed to the endorsement of OSI and accelerated its implementation. The OSI concept has grown into an international movement and it has evolved from an architectural framework to a set of specific protocols and functions profiles.

EC Policy on OSI and 1992. Information technology plays a key role in the completion of the single integrated internal market in Europe planned for 1992. The development of a unified IT market in the Communities requires the application of common harmonized standards ensuring the interoperability of equipment and the effective exchange of information among member states in a multivendor competitive environment. Accelerated diffusion of IT systems conforming to OSI standards constitutes an essential element of European economic integration.

The main features of the Communities' policy actions in this respect are:

- Promotion of, and support for, OSI standards in IT and of a competitive multivendor market
- Promotion of, and support for, the establishment of information technology and telecommunications (IT&T) conformance testing laboratories offering third party test services
- The mutual recognition of accredited laboratories test reports
- Promotion of public sector purchasing of OSI conformant systems
- Development of a common market for telecommunications services and equipment through the application of harmonized European standards offering equal opportunities to all market participants
- Increase in the Communities' technological capacity to a highly competitive level of collaboration in advanced research and development (R&D) projects among industrial partners and research centers
- Promotion of innovation and diffusion of new technologies into more sectors of the economy.

Standardization. The OSI standardization is at the heart of the Communities' IT standardization policy. Where needed, the Communities' policy calls for the production of European Functional Standards which are complementary to, yet consistent with, the international standards.

Sometimes known as profiles, a functional standard is a coherent way of deriving useful, functional systems from the OSI standards available. It selects a subset of basic standards and related options and parameters from the range of available options within OSI that meets a particular set of needs and is suitable for achieving a well defined function. At each layer of OSI, a number of choices should be provided to cover a wide range of needs. Such standards normally take the form of a superset covering a broad range. A functional standard may include some options but generally it is intended that all systems built to the standard will work together.

A major worry is that the work done by the international movement to open systems will be harmed by the creation of a range of different profiles. However, the disadvantages of a proliferation of bodies involved in functional standardization are outweighed by the practical solutions they offer when adopted. The European IT&T industry participates within European Standards Committee/European Electrical Standards Committee/European Conference of Postal and Telecommunications Administrations (CEN/CENELEC/CEPT) in the preparation of functional standards for all main data transfer and intercommunication functions.

The European program of OSI functional standardization constitutes a comprehensive plan for functional standards. The first set issued by CEN/CENELEC/CEPT covers mainly OSI-related areas such as the lower layers of the OSI reference model for private and public networks, and upper layer applications. The transport layer plays a pivotal role in the seven-layer OSI model. Above it, an application will demand services and below it, a communication medium will provide a particular set of services. An "application profile" refers to the top three layers, and a "telecoms profile" refers to the lower three layers of the model.

Current standardization work is concentrating on the application layer where application profiles such as File Transfer and Access Mechanism (FTAM) and Office Document Architecture (ODA) are being specified. The European Workshop for Open Systems (EWOS) within CEN/CENELEC brings together supplier based bodies such as the European Computer Manufacturers Association (ECMA) and Open Systems Interconnection Tech-

nical and Office Protocols (OSITOP). It provides input to CEN/CENELEC and promotes international convergence through contributions to OSI on the development of harmonized OSI functional profiles.

Key legal instruments for OSI are Directive 83/189/EEC and Council Decision 87/95/EEC. The former prevents the creation of new technical barriers in the Communities by requiring member states to serve advance notice to the Commission of all draft regulations and standards concerning technical specifications that they intend to introduce in their own territory.

Council Decision 87/95/EEC calls for work on European standards--functional standards--to fill the gaps caused by the lack of precision or the multiplicity of options or the ambiguities in the international standards; the need use standards in public procurement; and reference to European standards in national regulations.

Conformance Testing. The aim of conformance testing is to provide a base of discipline to the implementors and confidence to customers investing in OSI. The Conformance Testing Service (CTS) Program was launched by the European Commission in 1985 to promote information technology and telecommunications standards. The program has been phased in three overlapping stages, each launched through a call for proposals within 2 year intervals. Communities funding covers 50 percent of the cost. The very basic idea of the CTS Program is to enable conformance of IT products to standards based on the principles of independence, mutual recognition, and standardization. The practical rules are set out in Table 1.

Table 1. Conformance Testing Services Program.

- There should be one set of tests for any given technical area throughout Europe, and the tests should be internationally standardized.
- Every test service should be offered in at least two member states.
- The services should be made available regardless of the country of origin of the product.
- There should be mutual recognition of results among countries, at least within Europe and preferably worldwide. A product tested in one country should be accepted without retesting in another.
- There should be competition in the provision of testing services. The availability of alternative sources for the tests should act as a natural mechanism to avoid potential problems of partiality, unreasonable pricing or excessive waiting times.
- The tests should be grouped according to the needs of the procurer and hence, of the supplier. If conformance to several related standards is needed for the performance of a given user perceived task, then the tests should cover the full set of standards.
- Such multistandard testing services should cover the European functional standards and the international standards referenced therein.
- The testing services should become financially autonomous. Funding may be needed during the development phase and in an early period before a break-even point is reached, but not continued funding.

The actors in the CTS Program are the Commission of the European Communities, The Member States, The European Companies and Organization, and The Standardization Bodies. About 30 projects to establish services are underway which will lead to more than one hundred testing centers covering the various domains in the IT field. Current CTS services are shown in Table 2.

Table 2. CTS Services.

OSI Application MHS (P1 & P2 Protocols		Layers 4-7
		Layers 6-7
FTAM (single file transfer)		Layers 6-7
TELETEX		Layers 4 - 7
X.75		Layer 2
Intermediate layers TRANSPORT		cl 0,2,4
	SESSION	
OSI layers NETWORK	X.21 DTE	
	X.21 bis	Layer 1
	X.25 DTE	
	LAN CSMA/DC	Layers 1-4
Non-OSI specific services are available for		
Language Compilers	COBOL, FORTRAN, PASCAL	
Graphic Kernel System (GKS)		
Software Quality Assurance (SQA)		

Conformance testing refers to the test of a product against the requirement of a standard specification. On the other hand, interoperability testing refers to the verification that one or more products can interwork without conforming to any standard. Customers needing both should proceed as follows: conformance test, then interoperability test, then performance and robustness test.

Certification is essentially an administrative task of awarding the product a certificate when it satisfies the tests of conformity to the standards.

Council Decision 87/95/EEC says, "the field of public procurement orders is a suitable place to encourage wider acceptance of open systems interconnection information and data exchange standards through reference to them in purchasing. Under the Decision, Member States are now under the obligation to ensure that reference is made to: European standards and European prestandards; international standards when accepted in the country of the contracting authority; in public procurement orders relating to information technology, so that these standards are used as the basis for the exchange of information and data for systems interoperability."

Canadian OSI Initiatives, Michael Harrop, Senior Project Officer, Treasury Board of Canada. Several programs exist in Canada, at both the federal and provincial government levels, to encourage OSI-related research and development either by direct grants or by generous tax incentives. The federal government is a founding member of the Canadian Interest Group on Open System (CIGOS) which exists to promote the development and implementation of open systems for the benefit of Canadian users, suppliers, and carriers. The group was formed

in 1987, has 40 organizational members, and held its first annual conference and trade show in 1988.

Government OSI Policy and OSI Profiles. It is government policy that departments migrate to OSI by the early 1990s. A three-level committee structure has been established as part of the policy implementation. The Steering Committee of senior executives resolves key strategic issues such as staffing and funding. The Implementation Committee addresses general issues of implementation, coordination, and strategy. The Profiles Working Group is responsible for defining the actual profiles of standards to be used to achieve a particular task or to specify options or parameters of a specific standard to be used in a particular case. The most visible product of the implementation activity is the Canadian Open Systems Application Criteria (COSAC), similar to the U.S. and U.K. GOSIP. Its purpose is to help departments to migrate to OSI as quickly and painlessly as possible. Profiles have so far been developed for local area networks, message handling, and internetworking. Profiles in preparation include File Transfer, Wide Area Networking, and Security.

Innovative OSI applications have been developed in the National Library for bibliographic networks, in the Hydrographic Services Division of the Department of Energy, Mines and Resources to transfer map and chart information electronically, and the Canadian Aeronautical Digital Network to modernize the facilities and equipment of the Air Navigation System.

The International Conference on the Application of Standards for OSI drew 200 people from 14 countries for the 1987 conference in Bonn. In October 1988, a meeting of public sector OSI profile developers was held in Ottawa. Representatives from Australia, Canada, Japan, Sweden, the U.K., the U.S., and the Communities attended the meeting to examine possible ways of achieving greater alignment between profiles and collaboration on the definition of requirements. The group, now called the International Public Sector Information Technology Group (IPSIT), met in Tokyo in March 1989.

Future plans in Canada include: establishing an OSI Center for expertise and support; assisting Canadian industry in OSI product development; establishing and operating an internationally-accredited conformance test center for IT products in general and OSI in particular; fostering the development of advanced OSI product development tools and reducing the product development cycle time and cost; providing support to Canadian user groups, associations, and standards committees; and contributing to international harmonization efforts.

OSI and the French Regulations on VANS, Thierry Zylberberg, Mission a' la Reglementation, Ministere des PTE, France.

In order to meet the European deadline of 1993, the French government is taking active steps to promote the growth of VANS. It is necessary to open the market and to introduce fair practice rules. The VANS services based on switched telecommunications services are not subject to any regulatory constraints. The TRANSPAC, the Public Packet Switched Network, is the largest in the world with several thousand value added services available through Teletel videotext services. Also, at the end of 1987, the French government introduced a decree reforming the use of leased lines. This new regulation distinguishes between two statutory positions called regimes. The general regime allows direct connection of third parties to networks, provided they are identified and that the connection is unique. The newly created regime of "Reseaux Telematiques Ouverts a' des Tiers" (RTOT) allows the interconnection of private networks to public networks in several points. It forms the legal basis on which VANS services providers can operate. However, the regime applies also to companies or individuals that run networks for their own use and do not provide services to third parties on a commercial basis.

There are two constraints on the operator of an RTOT: (1) To prevent a simple resale, the service must provide a true added value above the simple transport of traffic. The ratio of the transport bill over the complete service revenue should not exceed a given value (initially fixed at 15 percent). This ratio can be increased and not decreased by a decree from the Minister of Postes, Telecommunications, et Espace (PTE) and (2) two thresholds separate the simple declaration (registration) from the Authorization (license) of the Ministry. These thresholds measure the size of the network by adding all the external accesses to the network. The threshold values are set at 3.5 Mbps for general services and at 5 Mbps for specific services. These ratios can be increased by the Minister of PTE.

Why an OSI Policy? Opening a market is a destabilizing process and deregulation must proceed at a measured pace. Also the VANS market is new, emerging, and thus unstable; and a constant monitoring of the effects of free market forces is needed. The end users need interconnectability and interworking; and OSI standards can help to fulfill the need.

The French Policy. The policy in France is to inform the actors as to the status of the OSI work, prescribe the OSI standards, and apply the prescriptions. To achieve the information objective, the French government, together with the Association Francoise de Normalistation (AFNOR), has established a large database of OSI documents that will enable anyone to find out which documents are relevant to a specific problem and to order these documents from the reference library.

On the matter of prescriptions, the Groupe Permanent Prescriptions Technique composed of some 20 people from Computer Manufacture, VANS providers, standards bodies, the academic community, research centers and government officials is responsible for the choice of standards, eventually prescribed by the Ministry of Posts, Telecommunications, and Space.

The big difficulty is that of applying the prescription. The method adopted is based on the CCITT standard cable LDS coupled with the method of structuring data along an *entity/relation* model. The basic idea is that any given service is a combination of generic elements assembled for a specific purpose and completed by some specific functionalities. The OSI standards only relate to the generic elements and not to the specific part of the service. The method states that there is a limited number of generic elements that can be similar to OSI elements or indeed outside the realm of the OSI process. It is then easy after decomposing a value added service into generic elements to identify which OSI standards are relevant.

Conformance Testing and Certification

Chairman, Jayant Gadre, Manager, Advanced Studies, COS International, U.S.

Current States of the ISP Taxonomy, Paul Jenkins, Head of Data Network and OSI Standards Group, British Telecom, U.K. In order to accommodate the urgency of functional standardization, new ISO procedures are being proposed so that documents can be published in a shorter time scale. To do this, it has been necessary to create a new type of ISO publication called an International Standardized Profile (ISP). Functional standards approved by ISO will be published as ISPs.

Joint Technical Committee (JTC) 1, cosponsored by ISO and IEC, is to promote international standardization in the field of IT. The Special Groups of Functional Standardization (SGFS) manages the program for the development of ISO ISPs on behalf of JTC1. It in turn has delegated the task of drafting the ISP framework, including taxonomy, to the Functional Standardization Taxonomy Group (FSTG). The Functional Standards Review Group (FSRG) reviews the proposed ISPs. The most significant base standards on which profiles will be based are: SC6-Data Communications, SC18-Text and Office Systems, and SC21-Open Systems.

These technical committees and special groups are made up of contributors from national standardization bodies that participate in the work of ISO and those that observe the work of ISO as well as liaison bodies such as CCITT.

The three broad classifications of profiles are those that deal with the structuring and coding of information, those that deal with the application and its communication needs, and those concerned with the use of network technology for interconnection. The latter two refer to layers 5-7 and layer 1-4 in the OSI concept.

The OSI Transport Service has been taken as the boundary between them. However, since ISO standards for OSI recognize two types of transport service, connection mode (COTS), and connectionless mode (CLTS). Consequently the above two classifications are each split into two, based on the type of transport service used for the boundary. This results in five profile classes:

- F Profiles-concerned with interchange and representation formats
- A Profiles-application profiles that assure the availability of connection mode transport service
- B Profiles-application profiles that assume the availability of the connectionless mode
- T Profiles-provide the connection mode transport service
- U Profiles-provide the connectionless mode transport service.

A Group is a set of T or U Profiles that are compatible, a system implementing one profile from the group can interwork, according to OSI, with another system implementing a profile from the same group. All the profiles within a group use the same type of Network Service.

The general framework within which the ISO functional standardization work will take place and the taxonomy is documented in an ISO technical report. Part 1 of the document provides the general framework for the taxonomy and gives guidance as to what kind of material an ISP should contain. Part 2 defines the current taxonomy and provides identifiers for the profiles the FSTG considers could be submitted for approval as ISPs. A document called the directory identifies those profiles in the taxonomy that are recognized as required by a submitting organization, those that are under development within a submitting organization, those that have been submitted to ISO and are under review or ballot, and those that have been approved as ISP.

It is likely that the taxonomy and the ISP approval procedures will be finally approved in 1989 and that the first ISPs may be approved in the second quarter of 1990.

Open Testing for Open Systems, Terence Holland, Head of Conformance Testing Standards and Development Group, British Telecom, U.K.

Much of the early work used the transport protocol as a vehicle for the formulation of conformance test methodology. Recently, the need to test application protocols has become more pressing.

In 1986, a group was established in CCITT to define abstract test suits for message handling services (MHS) based on the 1984 X.400 series of recommendations. Also in 1986, the European collaborative project (CTS-WAN) started, which was also concerned with MHS testing. However, the test notation proposed by the ISO group could not easily handle the more complex protocol data unit structures found in the application protocols. So the MHS, FTAM, directory, and other applications use the CCITT X.409 (or equivalent ISO ASN.1) presentation syntax.

A modular method was developed for refining protocol data unit values which was derived from the presentation style used in the X.400 series of recommendations for defining the protocol data unit syntax. This method

of defining constraints as well as the Tree and Table Combined Notation (TTCN) are now included.

The writing of abstract test suites has gone on in parallel with the development of the test notation. Consequently, some test suites are based on interim versions of the TTCN.

European Conformance Testing Services. The European Commission launched its CTS program in 1985/86. The OSI protocols are covered by two projects:

(1) CTS-WAN, covering telecommunication profiles for layers 1-4 and MHS, teletex and FTAM application profiles for layers 5-7 in the wide area network environment.
(2) CTS-LAN, covering telecommunications profiles for layers 1-4 in the local area network environment.

The CTS-WAN Project. This project is covered by four separate contracts with the EC involving the following subcontractors.

- British Telecommunications (BT)
- Centre National d'Etudes des Telecommunications (CNET)
- Centro Studi e Laboratori Telecommunicazioni (CSELT)
- Companice Telefonica Nacional de Espana (Telefonica)
- Deutsche Bundespost-Fermeldetechnisches Zentralamt (FTZ)
- Statens Teletjeneste, Telelaboratoriet (PTT-DK)
- The National Computing Centre Limited (NCC).

The four contracts are run under the control of a single Project Development Management Board. The project has been organized into six technical areas. The methodology technical area deals with issues common to all technical areas. The other five technical areas are: Network, Transport and Session, Teletex, Message Handling Services, and FTAM.

The methodology technical area provided guidelines for using the TTCN notation within the project; guidelines for protocol implementation conformance statements (PICS); guidelines for protocol implementation extra information for testing (PIXIT); relationship between abstract and executive test suites; method of demonstrating equivalence between test laboratories; maintenance of tests; and conditions of use of the CTS-WAN test services.

The test service consists of abstract test suites, protocol implementation conformance statement proforma, protocol implementation extra information for testing performa, and text report performa.

Future Work. There is much activity in ISO and CCITT to extend the range of protocols for which standardized conformance tests suites are available. Preparation is underway for five new international standards for OSI test suites:

- Full FTAM protocol testing
- ASCE protocol testing
- Presentation protocol testing
- Session protocol testing
- FTAM International Standard Profile testing.

The CCITT has already begun work covering X.400 messaging and X.500 directory services. They are identifying the documents required and defining the structure of the test suites.

Practical Experience in Setting up an Accreditation and Testing Scheme for OSI Products, Patrice d'Oultremont, Managing Director, SPAG, Belgium.

Setting up conformance testing requires activities ranging from political discussions or strategies assessment to selection of software quality assurance methods and the definition of data logging practices.

Building IT Certification Schemes. Two IT certification schemes of interest to IT vendors and users in Europe are (1) the European Systems for IT testing and certification under the guidance of the European Committee for IT Certification (ECITC) and (2) the Conformance Test Center Recognition project under the guidance of the World Federation of MAP/TOP User Groups (WFMTUG).

The European system will be based on three Recognition Arrangements (RAs) covering: software compilers (CCC-1), wide area communication protocols (OSTC), and local area communication protocols (ETCOM). The ETCOM (European testing and certification for office and manufacturing protocols) RA is the one test SPAG is actively promoting together with test laboratories. The open systems testing and consortium (OSTC) is a fallout of the CTS program funded by the European Commission.

One of the important objectives of ETCOM participants is to contribute to setting up a certification scheme by the WFMTUG. The ETCOM has generated, with the support of SPAG, significant inputs to the WFMTUG.

Accreditation of Test Laboratories. The required accreditation process for test laboratories will be undertaken by National Accreditation bodies using criteria established by a Recognition Arrangement within the ECITC scheme. A major part of the laboratory accreditation process will emphasize the Quality Assurance System. This takes the form of the definition of procedures to be included or references from a quality manual.

When the full infrastructure is in place, an internal audit program by the Quality Assurance Manager will assess conformance to the procedures. Concerning the test tools, emphasis is placed on ensuring the consistency and repeatability of test results.

The next step toward accredited status is a full internal Beta accreditation exercise. It may require several such exercises before a laboratory is sufficiently confident to apply to its National Accreditation body for accredited status.

The laboratories in the pilot phase, committed to providing conformance testing services are shown in Table 3.

Table 3. Conformance Testing Pilot Phase.

Laboratories	Service
ACERL1 (France)	Manufacturing message specifications (MMS) and the lower layers
The Networking Centre (UK)	Lower layers
Fraunhofer Institute (Germany)	MMS, DS and NM
KEMA (Netherlands)	Lower layers
SPAG (Belgium)	MMS, DS and NM

Experience Summary. The choice of staff is of prime importance; quality assurance manager is mandatory; air conditioning systems is needed to meet client requirements; appropriate documentation system is necessary; and control demands a disciplined filing system.

New Directions in OSI Conformance Testing, Dermot Dwyer, OSI Manager, Technical Development Program, National Computer Centre (U.K.).

As the work of the U.K. Consortium and CTS-WAN come to an end during 1989, NCC has identified two areas in which major development work is required--the extension of the testing process to some of the newer OSI protocols and support for interoperability and cost effectiveness in the design of test systems and test suites. Two projects in which we will attempt to extend the range of OSI testing are U.K. Consortium II and CTS2.

U.K. Consortium II. The two main goals of Consortium II are extending test coverage and maintaining cost effectiveness. The technical program covers work on both the X.400 message handling standards and the X.500 directory services standard. The program will also cover another protocol to be determined by the members of the consortium.

One problem with the standards-making process is the complexity and flexibility in the specifications produced. This occurs as a result of trying to achieve both technical and political consensus. In FTAM, an attempt to allow the maximum degree of flexibility in the description of file contents and file access techniques led to a standard that allows a great deal of freedom to the implementor in terms of options within the protocol and file attributes support. In some cases, these options cover trivial matters but in other cases the choices can influence the order of protocol events or the types of files that can be manipulated.

The above can be further complicated by the fact that the principle of freedom of options applies across the variety of specifications that make up the constituent parts of an OSI system. In principle, there are many ways that the different functional units that constitute the session or FTAM protocols can be put together and there is little or no guarantee that dissimilar implementations of the same protocol specification will support the same elements of procedure.

Work to remedy the above situation has been done in three areas: (1) defining functional profiles and functional standards; (2) establishing testing systems and services to verify the compliance of real end systems to the profiles outlined above; and (3) establishing certification and accreditation to control the testing process in terms of the procedures and test cases to be applied as well as the monitoring of results.

Functional Profiles. A functional profile is an extra set of constraints imposed on an implementor in addition to those imposed by the OSI standards. Using a functional profile allows session layers to be tailored to the environment in which they will operate and the application they will support. Similarly, the scope of a file transfer application may be reduced if extra restrictions can be imposed on the way it is used.

Adopting a functional profile should increase the chances of interworking between dissimilar systems over and above that supplied by the base standards. However, a plethora of functional standards can create islands of interworking separated by dissimilarities in the profile and can add to the confusion in the OSI market rather than reduce it. Thus, there is a need to bring together some of the different profiles to make them compatible and there is considerable effort underway to do this.

Testing Systems and Services. Experience in testing has led us into the development of test cases and test software. Three projects stand out--the U.K. Consortium; the European CTS-WAN project; and involvement with COS. The U.K. Consortium includes both industrial and development members with representatives from British Telecom, DEC (U.K.), IBM (U.K.), ICL, and the National Physical Laboratory. Test systems and test cases have been developed for ISO session and FTAM protocols used by the industrial members and to provide a testing service by NCC.

The European CTS-WAN project, sponsored by the European Commission, is an attempt to harmonize test cases, procedures and result analysis across Europe. The main contractors are British Telecom and NCC in the U.K. and the PTTs of France, Germany, Italy, Spain, and Denmark. Testing must be done to functional profiles rather than to base standards.

The final major program of work on OSI conformance testing involves NCC and COS. The NCC has provided COS with technology to test implementations of the OSI transport protocol and has been involved in the development of the COS, FTAM, and MHS test systems that are targeted toward the NBS implementors agreements and subsequently to International Standard Profiles.

Certification and Accreditation. Certification has existed for some time for COBOL and FORTRAN compilers and the testing of Ada compilers recently has led to the general impetus toward certification in the IT industry. Along with certification is accreditation that particular laboratories are qualified and controlled to

perform the test for certification. Also, the U.K. Consortium will further develop the NCC OSI monitoring system to provide an interoperability tool applicable to a wide variety of OSI applications operating over a variety of lower layer support stacks.

The CTS2 program is a followon from CTS-WAN and addresses enhanced harmonized test services for FTAM, X.400, X.500 and ISDN. The emphasis will be on tests and services rather than technological advance.

Cost Effectiveness. There are two fundamental mechanisms being used to make testing more cost effective: the application of software engineering techniques to the design and construction of test systems to make them cheaper to produce, configure, and use; and an analysis of the test suite production.

Standards Issues I: Management and Security

Chairman, Alwgn Langsford, Network Manager, Harwell Laboratory.

Modeling Management Functions in OSI, Ole Thomsen, Software Engineer, Jutland Telephone, Denmark.

The purpose of OSI Management standards is to provide the means for Network Management. To manage a network, one needs tools to access equipment from different manufacturers, placed at different locations. This can be achieved by having a communication standard for exchange of management information which offer services to support the differing management functions required to manage the network. It is the aim of working group 4 in ISO to specify and publish these standards. The different forms of management are: (N)-layer operation is the normal use of (N)-layer to provide the service for which it is intended; (N)-layer management is supported by a special (N)-layer management entity that provides facilities for exchange of management information at the (N)-layer; and Systems Management is the normal method of exchanging OSI management information. Systems management communication takes place between application processes (layer 7). So systems management is based on exchange of Systems Management Application Protocol Data Units (SMAPDU). These units are exchanged by use of supporting application layer services such as the Common Management Information Service Element (CMISE).

Systems Management Model. Systems Management is based on an object-oriented model. Systems Management is described in terms of operation on and notification from things called management objects. A managed object is the OSI Management view of a resource within the OSI environment that may be managed through the use of OSI management protocols. So the managed object model is part of the OSI environment and the model is standardized in the SMI standard.

Real management information is represented and stored in a real open system according to local implementation requirements. However, when management information is communicated, it is done in terms of the model. Two different kinds of managed objects exist. For example, an (N)-layer managed object may be a Network-layer managed object which will typically consist of a Network-layer entity containing network protocol entities as managed objects which in turn may contain virtual circuits as managed objects. On the other hand, systems managed objects are managed objects that are necessary to support systems management which do not belong to a specific (N)-layer. An example is a LOG-managed object which contains log records and filters as managed objects.

In the SMI standard, another hierarchical structure of managed objects is called inheritance hierarchy, which is used to define generic managed object classes.

System Management Function. In the OSI reference model the term (N)-function is defined as a part of the activity of (N)-entities. So a systems management function is merely a name of a subdivision of systems management activities. The reason for using the term systems management function is to allow standardization of systems management to be divided in logically independent and self-contained documents. A systems management function will correspond to a service which will meet the needs of a user. Systems management function areas (SMFAs) meet user requirements like fault management, configuration management, security management, performance management, and accounting management.

Some systems management functions have been standardized with the standard containing user requirements; models employed to define functions that meet user needs; lists of OSI systems management services required for each function; abstract syntax definition required to specify the parameters defined in these services; mapping of these services to supporting services; and functional units used for negotiation.

Relationship Management Function. A relationship is a set of rules that describe how the operations of one part of an open system affects the operation of another part of the open system. The concept of relationship is introduced to allow the handling of interdependencies among managed objects. An example is the service relationship in which one (N)-layer entity (A) is the service user of another (N-1)-layer entity (B), which through the same relationship is the service provider for (A).

Error Reporting and Information Retrieval Function. The requirements to be satisfied by this function are reporting of occurrence of errors and information relating to errors, and retrieval of accumulated statistics on the occurrence of errors. The model developed for this function contains concepts of error types and error severity.

The systems management functions identified thus far are for object management, state management, relation-

ship management, error reporting and information retrieval, management service control, confidence and agnostic testing, log control, and software management.

NATO OSI Security Architecture, Nicholas Neve, Scientist MOD, Royal Signals and Radar Establishment.

The NATO has for many years produced its own standards, called standardization agreements (STANAGs) covering a wide range of military equipment, procedures, interfaces, and the way information is to be exchanged between formations. The primary concern of NATO is to achieve interoperability between both the command, control and communication systems of the individual member nations and also between those systems and NATO's own command systems.

The NATO interoperability management plan (NIMP) is the high level policy document setting out NATO's plan to achieve greater interoperability. Services that are required to interoperate are: reporting, data exchange, remote servicing, electronic mail, and conferencing.

The NATO Technical Interoperability Standards (NTIS) specify the functional, electrical, and physical characteristics of equipment for information exchange. These standards are to be developed in accordance with a NATO Reference Model of Open Systems Interconnection which shall adopt the ISO Seven Layer Reference Model for OSI as its basis. The NATO model will include military enhancement for multihommed and mobile host systems, multi end-point connection (multiaddressing), internetworking, network or system management function, security, robustness and quality of service, precedence and pre-emption, and real time and tactical communications.

The NATO has studied the ISO OSI security architecture (ISO 7498-2) and has concluded that it forms a suitable basis for providing the NATO OSI security architecture. However, since ISO 7498-2 contains too many options for NATO's purpose, NATO has selected a subset of the OSI security architecture options and is presenting them in a form consistent with NATO requirements.

Placement of Security Services. The OSI security services identified by NATO for the physical layer are:

- Connection confidentiality. Connection confidentiality at the physical layer must be capable of dealing with circumstances where the physical communication is intermittent or asymmetric.
- Traffic flow confidentiality. These security services can be provided by transparent means and no protocol modifications are required. No OSI security services have been identified by NATO for the data link layer.

The OSI security services that can be provided for individual sub networks and those that can be provided for NATO interoperability within a *trusted communications sublayer* of the network layer have been separately identified in subparagraphs (a) and (b).

(a) Subnetwork dependent roles. A number of OSI security services which may be required to be provided over individual subnetworks have been identified by NATO as follows peer entitity authentication, data origin authentication, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity.

The above are not considered to be prime candidates for NATO interoperability standardization since they operate solely across individual subnetworks.

(b) Trusted communications sublayers. The trusted communications sublayer comprises self-contained security functionality that provides a thread of commonality of security services and security mechanisms between national systems in the NATO community. In this sublayer, self-contained security mechanisms will be invoked before the relay and routing functions of the network layer on transmission and after the relay and routing functions on receipt. It will provide the functions listed in paragraph (a) above.

The NATO realizations of the trusted communications sublayer will be special equipment which is designed, implemented, certified, and distributed under strict NATO control.

No OSI security services have been identified by NATO for the transport layer or the session layer.

A number of OSI security services will be provided to application processes in the application and presentation layers. They will be invoked by the application process and realized by an appropriate combination of security mechanisms operating within these layers.

The OSI security services identified by NATO that can be provided by the combinations of the presentation and application layers are presented in Table 4.

Table 4. OSI Security Services.

- Peer entity authentication
- Data origin authentication
- Access control
- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality
- Connection integrity with recovery
- Connection integrity without recovery
- Selective field connection integrity
- Connectionless integrity
- Selective field connectionless integrity
- Nonrepudiation with proof of origin
- Nonrepudiation with proof of delivery

Standard Issues II: Naming, Addressing, and Directories

Chairman, Jon Stranger, Senior Consultant, CCTA.

OSI Naming and Addressing: Principles and Conventions, Gunnar Almgren, Research and Development Engineer, Swedish Telecom, Sweden.

The ISO/OSI naming and addressing model builds on well-known concepts from other network architectures but also introduces some new concepts and definitions. In some earlier network architectures like Arpanet (TCP/IP) protocol suite, there has been a significant difference between the notions of the name and an address. The OSI model puts no restrictions on the language used to define names, thus obscuring the difference between names and addresses. In OSI, addresses are just a special kind of names.

The OSI model partitions the name space into a hierarchy of independent naming domains. For each domain, there is a naming authority that allocates names to all of its subdomains and/or the relevant network objects under its administration. Thus, all names will be globally unambiguous. However, two different names can be bound to the same objects.

The most important properties of an address are the syntax and the semantics. Each address usually has an abstract syntax and a concrete syntax. The abstract syntax is the representation used when writing or talking about the address. The concrete syntax, or encoding, is the representation of the address when transferred as a bit stream on a transmission line. The semantics of an address is the meaning assigned to it, and should be independent of the particular concrete syntax chosen for the address.

OSI upper layer addressing. The addressing mechanisms used in the upper layers of OSI (transport, session and presentation) are basically the same in each layer. A selector mechanism is used to identify the service user; i.e., the entity in the layer above that is using the protocol. The protocols in these layers do not provide any means for naming. The OSI applications are identified by presentation addresses consisting of a triple of P-selector, S-selector, T-selector, and a list of network addresses, typically only one.

Naming in the application layer. The OSI uses quite different structures to identify users and application processes. An application process (AP) is an abstract representation of those elements of a real open system that perform information processing for a particular application. The aspects of an AP that need to be taken into account for the purpose of OSI communication are represented by one or more application entities. Specific instances of the use of these entities are called application process invocations and application entity invocations.

OSI network layer addressing. There is a difference between network addressing and subnetwork addressing. Network layer standards recognize the existence of real subnetworks that may or may not represent the full OSI network service. A subnetwork address is the information that a real subnetwork needs to identify some piece of equipment attached to it.

The reference model imposes three basic requirements on network layer addressing. Every network layer address should be globally unambiguous; i.e., every network address should identify only one set of network service access points (NSAPs) in one end system (typically this set of NSAPs will have only one member). One NSAP may have several (synonymous) network addresses, although this is generally undesirable. Network addresses should also be globally applicable. Another requirement is route independence. Network service users should not be able to derive routing information from the network address, nor influence the service provider's choice of route by means of network address.

All the NSAP formats defined by ISO follow the domain addressing principle. At every level in the domain hierarchy, an initial part of the address unambiguously identifies a subdomain and the rest is allocated by the authority associated with the subdomain to unambiguously identify either a lower level subdomain or an NSAP within the subdomain. The NSAP address consists of the initial domain part (IDP) and the domain specific part (DSP). The IDP identifies the subdomain of the global addressing domain and the addressing authority responsible for address allocation within the subdomain. The DSP is the corresponding subdomain address. The IDP can be subdivided into two components--the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI). The AFI contains several kinds of information: specifies the format of the IDI; identifies the addressing authority responsible for allocation value of the IDI; specifies whether leading zeros are significant in the encoding of the IDI; and identifies the abstract syntax used to describe the DSP.

The Directory - Existing Services and Proposed Enhancement, David Chadwick, Senior Research Fellow, IT Institute, University of Salford, U.K.

Directory objectives that have been achieved are provided in Table 5.

Figure 5. Achieved Directory Objectives.

- The directory is based on existing OSI protocols and provides the directory capabilities required by most, if not all, OSI applications and telecommunications services. It is not application specific and has a wide range of applicability.
- The directory may be distributed between as many different systems over as wide a geographical area as required, or may be located in a single system at a single site.
- The result of a directory query will not depend upon the location of the enquirer.
- A global naming scheme has been defined as user friendly.

However, some important objects have not been met, primarily because the time constraints imposed by the CCITT four year study period, which ended in 1988. These are now the subject of work on addenda or additional parts to the base standard to be completed by 1992. See Table 6.

Table 6. Unachieved Directory Objectives.

- Support for replication of the information held by the dictionary
- Standardize access controls on the information held by the directory
- Specify the procedures that will allow for any information held by the directionary to be modified
- Support for alternate name forms that are either shorter or more user friendly.

Distributed Aspects of the X.500 Standards for Directory, Sara Radicati, Senior Product Planning Manager, Xerox, USA.

The OSI directory (CCITT X.500/ISO 9594) is a distributed system designed to support the name to address binding requirements of OSI applications in a distributed network environment. The directory holds information about OSI users and network resources in the form of database entries composed of a name and network resources in the form of database entries composed of a name and a set of attributes. The name of each entry serves to uniquely and unambiguously identify an entity in the OSI environment. The attributes associated with each entry further qualify the OSI entity by providing additional information pertinent to its use. The most fundamental attribute associated with entry names is the entity's OSI network address. Knowledge of this address allows OSI entities to communicate with each other. The directory performs a central role in OSI communications by binding names of entities with their addresses, and providing a single, unified name space within which all OSI entities are identified. The directory also provides location independence of network entities in the OSI environment.

The collection of information held in the directory is called the directory information base (DIB). The DIB may be either centralized in a single network node or distributed over a collection of nodes. Users of the directory, either people or application programs, can access the directory through a directory user agent (DUA) that cooperates in holding the DIB and provides users with a unified set of services. The directory standard specifies two protocols: (1) directory access protocol (DAP) used by DUAs; (2) directory system protocol (DSP) used among DSAs to cooperate in providing the directory service.

The standard models the directory environment in a object oriented manner, as a directory object, that can be further refined in the distributed case to comprise several DSA objects.

In relatively small network environments, where the DIB is fully contained in a single DSA, the directory is centralized and its operation is essentially defined by the DAP protocol. However, as OSI networks mature, this scenario is likely to evolve rapidly to a situation where the DIB is too large to be contained in a single DSA and must be partitioned over a set of DSAs.

The paper deals with the distributed aspects of the directory service, the manner in which DSAs interact with each other, the mechanism for partitioning DIB information over multiple DSAs, and in a distributed DIB. Some techniques are presented to facilitate the efficient operation of distributed operations, and a discussion is given on how the present information distribution mechanisms may evolve in the future to support replication of information.

Standard Issues III: Recent Developments

Chairman: David Firnberg, Chairman, DFA.

OSI in a Multilingual Environment - The Multiple-Octet Character Set Code, Marjeta Pucko, Research Institute Josef Stefan, Yugoslavia.

In OSI, an application is identified as an automation with two types of active entities--User and Automation. These two entities may be involved in one of the following relationships: User/User, Automation/Automation, and User/Automation. User communicates with the Automation by issuing commands and data and vice versa, and applications with the users by requirements for information and execution reports. The dialogue is based on written (textual) information and its presentation must be hardware independent, based on natural language and unambiguous.

The connection oriented presentation layer is restricted in choice of character set code to: ISO 646 (IRV), ISO 6937 (part 2), and ISO 8859 (parts 1-8). The ISO 646 is a 7-bit code like 7-bit ASCII except for currency and dollar sign. The other two codes are 8bit and their character set repertoire allows for the alphabets of more than 20 languages spoken in Europe, and North and South America.

The presentation layer and the accommodation of the coding. There are four ISO standards associated with the presentation layer: ISO DIS 8822 service definition, ISO DIS 8824 ASN.1 notation, ISO DIS 8823 protocol specifications, and ISO DIS 8825 ASN.1 encoding rules.

The first two specify the service and protocol to support the presentation layer and the second two are tools that support the presentation layer view of data. The ISO 8824 specifies a notation for the definition of abstract syntaxes enabling application layer standards to define the

types of information they need to transfer. The ISO 8825 defines a set of encoding rules that may be applied to values of types that are defined using the notation of ISO 8824.

The presentation layer and the associated standard documents are dedicated to solving the communication problems of two application layer entities that are different concrete syntaxes. The abstract syntax defined in ISO DIS 8824 and 8825 enables the definition of an application layer data structure independent of its representation. The presentation layer provides the transformation between the syntaxes of the application layer entities and the common syntax needed for communication. An abstract syntax is defined as a collection of data values with associated meaning regardless of any specification of how they are represented in binary octets. Examples of abstract syntaxes are: integer, Boolean, bit string, octet string type, sequence of IA5 characters, and floating point number.

The recommendation CCITT X.409 defines a defined type of string characters as a type specified by using the standard notation for type definition. The current version of X.409 containing seven defined types is presented in Table 7.

Table 7. CCITT X.409 String Characters.

- IA5 string (characters from the international version of alphabet No.5 or ISO 646)
- Numeric string (a set of characters that encode numeric information in tactual form)
- Printable string (characters chosen from the subset of printable character)
- T.61 string, a T.100 string or ISO 6937 (1/2/3/4) string (eight bit coded control and graphic character set suitable for Teletex and Videotex)
- Generalized time according to ISO 2014, ISO 3307, and ISO 4031
- UTC time type that is a generalized time especially suited for message handling system (MHS) application.

The 8-bit code. The character set of the IA5 alphabet or the 7-bit ASCII covers only the repertoire of the English alphabet. The character set adopted in the documents T.61 and T.100 or ISO 6937 are intended to be used in services offered to the multilingual environment of Europe and North and South America. The same coding was planned to serve for identified transliteration with non-Latin alphabets as well. The encoding rules of ISO 6937 comprise two different character sets in octet. One part of the character set (the left hand side of the code table) is the international version of ISO 646.

The second set, located on the right hand side of the code table, contains a column of nonspacing accents, which when combined with an immediately following letter, are used to give a two-octet representation for the accented letters of the Roman script. The repertoire of ISO 6937 defines 333 graphic characters and can represent text in about 40 languages spoken in Europe and North and South America.

The Multiple Octet Code. The implementation of the encoding described above are still deficient in some respects:

- No facilities for very large character sets
- No stable coding of characters (the same graphic character or the same command may have more than one code)
- Different coding techniques
- Variable length coding especially if more than 190 characters are involved
- No application in the world of ideographic alphabets
- Small repertoire even for Europe.

The development of the multiple-octet code is a task of ISO/IECJTC/SC2/WG2. The work on the character allocation in the multiple-octet code is in progress and a solution is expected in the near future. It is likely to have universal acceptance in the computer world similar to that of 7-bit ASCII. A special ISO number has been requested for the standard document; i.e., ISO 10646.

ODA-Applications, Implementations and Conformance Testing, Richard Carr, Deputy Principal Consultant, National Computing Centre, U.K.

The ISO TC97/SC18 has been developing an international standard for ODA and interchange format since 1981. The ODA provides for the representation of documents in two basic forms. Formatted form documents can be interchanged when the originator requires the recipient to lay out the document exactly and processable form documents can be interchanged when the originator wants to allow the recipient to revise the documents.

The model separates the logical structure with elements like chapter, author, paragraph from the layout structure with elements like page and column from the type of content (character, raster, geometric) that is shared by both structures. This allows future content types to be added.

The ODA is based on an object oriented architectural model that views a document as a set of objects with each object consisting of a set of attributes. As an example, an ODA document could contain a logical object paragraph with the attributes first line indented, right margin offset equal to X units, and protected. An ODA document might contain a layout object column with the attributes position, dimensions, and border.

The content models used by ODA are based on ISO 6937 for character content architecture, CCITT.4, T.6 and a *bit map* encoding for the roster graphics content architecture, and ISO 8682 for the geometric graphics content architecture.

Work is underway on extension to ODA for the inclusion of color and grey scale; interchange of document fragments; data in documents for business graphics and spreadsheets; extended typographical quality, security,

annotations, hypertext, automatic indexing and cross referencing; remote editing; and forms.

Document Application Profiles. Document application profiles are under development in various organization and are being harmonized through joint meetings and through the Profile Alignment group on ODA known as PAGODA. (See Table 8.)

Table 8. PAGODA Profiles.

Level 0	-	Simple messaging (UKGOSIP SMP EWOS Q121)
Level 1*	-	Basic wordprocessing (UKGOSIP GDAP, EWOS Q111)
Level 2*	-	Extended wordprocessing with graphics (EWOS Q112, CITT PM2)
Level 3*	-	Desktop publishing (NISTIA, INTAP AE1125)

*Available end 1989

Implementation. A number of vendors, including Xerox, Unisys, Wang, and Philips, are actively involved in prototyping interworking using ODA or are planning such activities. Two particular activities are described herein.

ESPRIT-PODA. The Piloting of ODA (PODA) project of ESPRIT has four participants--ICL, Siemens, Bull and Olivetti--and gave a demonstration of interworking at the 1987 Hannover Fair using equipment from each manufacturer. The demonstration allowed the interchange of processable documents containing such logical features as automatic section numbering, paragraphs, footnotes, and footnote references. At the 1988 Hannover Fair, the PODA group had been extended to include Oct of the Netherlands. The 1988 demonstration added raster and geometric graphics and used X.460 to transfer the documents. At the March 1989 Hannover Fair, the group had been joined by IBM (Germany), British Telecom, University College London, and Nixdorf (Germany).

NSF EXPRES. In 1986, NSF (U.S.) gave a three year contract award to Carnegie Mellon University and the University of Michigan for experimental research in electronic submission (ESPRES) to promote the electronic interchange of multimedia documents among the research community. A number of vendors provided equipment and technical support including DEC, Appolo, Sun, IBM, McDonnel Douglas, and Apple. In December 1988, the group demonstrated interworking at the AMC Conference on Document Processing Systems. They interchanged character text with mixtures of fonts, and raster documents between the Carnegie Mellon Andrew Toolkit, the Michigan University Diamond Multimedia system, and Interleaf. They also demonstrated an ODA to Troff translator. The output of the project will be a public domain ODA Toolkit that contains support for BSD UNIX, System V UNIX and MS-DOS, and for VAX/VMS and Macintosh.

Conformance Testing--the TODAC Approach. The testing ODA conformance (TODAC) project is a joint venture between the Canadian Government Department of Communications and the U.K. National Computing Centre. Other collaborators are USNIST (formerly NBS), British Telecom, and IDACOM (Canada).

The objective is to provide test tools and procedures for test services configuration to document application profiles based on ODA. The project will provide test definitions, test tools, and subsequent testing services.

An Overview of the OSI Transaction Processing Standard, Tony Fletcher, Head of Open Systems Communications Group, British Telecom.

There are several different styles of communication. For non real time store-and-forward in OSI there is the message handling system MHS (X.400) and the message oriented test interchange system MOTIS (OSO 10021). Real time bulk data transfer is handled by teletex, data transfer, access and management (DTAM T.500) and file transfer, access and management (FTAM ISO8571). Until recently, there was no support in OSI for the real time interactive, reliable style spanning two or more systems. This is where OSI transaction processing fits in.

Work in European Computer Manufacturers Association (ECMA) and elsewhere on transaction processing (TP) protocol for OSI has been in progress for several years. The CCITT has recently approved a new question which includes TP for OSI, but the major activity at present is in ISO/IEC. In March 1988, OSI TP became official as a three-part standard--model, service, and protocol. The work is expected to reach draft international standard (DIS) status in October 1989.

It has been agreed internationally that a subset of IBM's advanced program-to-program communications (APPC) verbs are analogues of a subset of the OSI TP primitives. This commonality at the service level should ease the writing of application programs that can run over APPC or OSI TP. However, the underlying protocol support is different.

A transaction in OSI terms is defined as a unit of work characterized by the Automicity, Consistency, Isolation, Durability (ACID) properties. Atomicity means all or none of the operations are performed; consistency means performed accurately, correctly and with validity; isolation means partial results are not accessible outside the transaction; and durability means the effects of a completed unit of work are not altered by failure of any kind.

The services offered by TP are divided into a number of functional units. The kernel provides dialogue control, error handling, and data transfer services. It must always be selected. The data transfer service is a dummy service that is used to represent the points in the sequence of TP services in which user protocol services can be substituted.

Shared control is the style of operation in which both partners in a dialogue can simultaneously invoke services.

In contrast, polarized control is the style in which only certain primitives can be issued simultaneously.

The handshake services can be used to synchronize the two partners. The commit functional unit provides the services to commit or rollback a provider support transaction. The heuristic services allow a node that has entered the ready state to unilaterally commit or rollback if it has to wait an unacceptably long time before receiving a commit or rollback command.

The unchained transaction functional unit may be used with the commit functional unit to allow a superior to exclude a transaction subtree from one a more provider transactions, and then to reinclude the direct subordinate.

The dialogue resumption functional unit is not currently a normative part of the standard, and is still being developed.

Mapping APC to OSI TP, Clive Partridge Technical Consultant, Data Connection (U.K.).

The APPC is IBM's strategic communications service. It is available on most IBM hardware platforms, and many other vendors offer APPC in order to participate in the IBM market place. It is a key part of IBM's proprietary communications architecture, called Systems Network Architecture (SNA). In addition to providing transaction processing capability, it is also the base for other SNA-based architectures.

Many users are seeking to replace their network based on proprietary protocols like SNA with those based on OSI, in order not to be vendor dependent. But this must be done in a way that preserves their investment in existing applications.

A major obstacle standing in the way of OSI is the cost for users to migrate from their existing networks. A significant part of the cost is altering applications to work with the OSI network. That cost is removed if applications can be migrated without modification. The objective of maping APPC to OSI TP therefore is to provide an APPC service from a network providing an OSI TP service. Applications can then be written to work interchangeably with networks based on OSI or on APPC.

Mr. Partridge's paper examines how an APPC network can be replaced by an OSI network that uses the OSI TP service, together with an additional application service element (ASE) to provide applications with the required APPC service. He then discusses how such a mapping could be expanded to a full gateway between on OSI and an SNA network.

A Practical Migration to Open Systems, Paul Frost, OSI Manager, Employment Department, Training Agency, U.K.

Mr. Frost's paper covered the rationale for moving to OSI protocols and the management issues surrounding the choices for implementation of OSI applications. Frost provided a view of the methodology used for determining the migration route to full open systems interworking at both networking and application levels, especially for those stable OSI standards where products are emerging or are being developed. Frost concluded with a view of the future issues that will need to be addressed and the possible future protocols that will be required for the major in-house applications systems.

The overall strategy is to introduce OSI throughout the organization to allow the communications needed to meet the business requirements. The tactics are the introduction of a corporate network and a corporate approach to the need for communications especially external communications, the introduction of services giving a substantial and fast payback, the introduction of services that reduce the reliance on specific suppliers and a strategy identifying the services that will be required to meet the business objectives.

Originally, four services were identified that were deliverable over a relatively short time from a number of suppliers and required suppliers wanting to sell equipment to the organization to commit to the provision of those services. The standards currently in draft form were identified that would enable provision of better or more comprehensive OSI services across the network either to system users or system providers. A decision was taken not to become involved with standards which cannot provide a reasonable payback.

The commitment to OSI is recognized by potential suppliers, project teams, and senior management. This enables the company to help direct OSI developments of suppliers rather than wait for product announcements. This also helps to plan the introduction of OSI into project implementation plans.

OSI Migration Problems in Strategic Networks, Nicholas Yannacopoulos, Senior Consultant, Computer Science, U.K.

Networks used by large numbers of user communities have evolved over many years as multi-vendor environment without recourse to OSI. In migrating such networks to OSI, a number of technical problems arise in the areas in interworking, fallback, security, and network management. Distributed applications introduce more technical problems than centralized ones, largely as a result of more complex interworking requirements, interdependence, and a larger variety of components used. The advent of broadband technologies and ISDN contribute to the fundamental difficulty of defining clear and realistic targets for OSI migration plans. Migration from a conventional network management to one conforming to the OSI management framework is nontrivial. The migration strategies used in simple networks require enhancement.

The term strategic network generally refers to large networks consisting of various types of subnetworks offering services to many user communities and supporting many centralized or distributed applications.

In current strategic networks that support distributed processing, interworking is often supported by means of

proprietary gateways internal or external to the end systems. However, the gateway and public protocols are not necessarily supported by the same versions of the operating system that supports OSI. This poses difficulty in migration because it eliminates the flexibility of carrying out the migration per system or per application.

The main advantage of gateways over OSI is that, in general, they do not require changes in the end system and, subject to physical configuration limitations, they can be retrofitted into almost any network. The man disadvantage is the reduced functionality in the areas of security, network management, and possibly addressing. Also, there is a lack of clear definition of their function in OSI terms and there is performance degradation or extra cost. However, temporary use of gateways is a practical migration alternative to single stage transition.

The Migration to ISDN

Migration to ISDN will implement OSI layers 1 to 3 of OSI for wide area networking. This is insufficient in strategic networks, since most of the switching is done in local area networks (LANs) and private branch exchanges (PBXs). The LAN interfaces to ISDN have not yet been standardized any further than defining the ISDN sides of gateways as ISDN terminals. The interconnection between LANs based on FDDI or FDDI2 requires broadband ISDN. Technical problems of migrating to ISDN strategic networks largely based on broadband backbones interconnecting broadband or narrowband LANs have not been solved in their entirety. The emergence of ISO open distributed processing standards, potentially biased towards the client server model, will make LANs popular for widely distributed applications and create the need for urgent standardization of LAN-WAN interworking units.

Migration of the Network Security. Complex security requirements increase the need to standardize by defining security in OSI terms before planning the migration to OSI, as well as the need to seek network solutions based on a widely accepted industry standard for the implementation. The ISO OSI Security Architecture and the U.S. DOD Red Book are useful reference documents, but they do not give guidance on implementation. The implementation of compatible options can only become a reality through the promotion of functional standards on security to which the manufacturers will conform.

Migration of Network Management. It is not possible under a regime of fragmented responsibility to achieve true end-to-end management as the users would wish. However, most strategic networks have in place a complex system of subnetwork management and end system management systems, often knowledge based, that are bound together with procedures and professional disciplines to provide an acceptable substitute for end-to-end management.

The migration to OSI management may benefit from ISDN. Standardized signaling between customer equipment and ISDN exchanges enables the implementation of mechanisms for ISDN to provide management data about the state of the subnetwork and the connections through it, for use by an end-to-end management system.

The Migration Process. The migration process will have to address the definition of migration communities, the selection of meaningful plan milestone, and the management of intermediate configurations. It will also have a number of management issues such as the funding for the migration, the preservation of the desired SOS during migration, and the education and training of users.

Under certain circumstances, gateways may be introduced as migration aids. Systems that are not intrinsically open may be equipped with appropriate gateways that make them appear to be open, at least to peers that have already migrated to OSI. However, this approach is neither universally applicable nor cost effective.

The project management challenges presented by the migration of strategic networks are quite significant and include the re-education of system developers and users, the preservation of acceptable quality of service during migration, and the maintenance of continuous and adequate funding.